

UNITED STATES DISTRICT COURT

for the
Western District of Washington

In the Matter of the Search of
*(Briefly describe the property to be searched
 or identify the person by name and address)*
 12123 2nd Drive Northeast, Marysville (Tulalip),
 Washington 98271 (Subject Premises), and David
 Paul Meats Jr, DOB 1999 (Subject Person)

Case No. MJ19-151

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

The Subject Premises and Subject Person as further described in Attachment A, which is attached hereto and incorporated herein by this reference.

located in the Western District of Washington, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B, incorporated herein by reference.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☒ evidence of a crime;
☒ contraband, fruits of crime, or other items illegally possessed;
☒ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section

Title 18, U.S.C. § 2252 (a)(2)
 Title 18, U.S.C. § 2252(a)(4)(B)

Offense Description

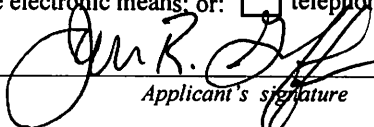
Receipt or Distribution of Child Pornography
 Possession of Child Pornography

The application is based on these facts:

- ☒ See attached Affidavit continued on the attached sheet

- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

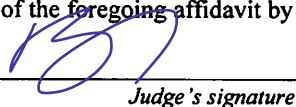
Pursuant to Fed. R. Crim. P. 4.1, this warrant is presented: ☒ by reliable electronic means; or: ☐ telephonically recorded.


 Applicant's signature

SPECIAL AGENT JASON R. GRAEFF, HSI
 Printed name and title

- ☒ The foregoing affidavit was sworn to before me and signed in my presence, or
☐ The above-named agent provided a sworn statement attesting to the truth of the foregoing affidavit by telephone.

Date: 04/12/2019


 Judge's signature

City and state: SEATTLE, WASHINGTON

BRIAN A. TSUCHIDA, Chief United States Magistrate Judge
 Printed name and title

ATTACHMENT A**Description of the Property to be Searched**

a. The physical address of the SUBJECT PREMISES is 12123 2nd Drive Northeast, Marysville (Tulalip), Washington 98271 . The SUBJECT PREMISES is more fully described as the property containing a one-story single-family home with a daylight basement. The Snohomish County Assessor's and Google Earth web search of the property reveal that the residence structure appears to have a first or main story that is approximately 2614 square feet with the basement or daylight basement of 2616 square feet. There is a three-car garage located to the right of the main door or at the southwest corner of the residence. The Snohomish County Assessor lists the garage being approximately 864 square feet. Google Earth shows the daylight basement with possible access to the backyard located on the east side of the residence. There appears to be a large deck coming out from the main floor. The SUBJECT PREMISES is located at the east side of 2nd Drive Northeast. The SUBJECT PREMISES has a long driveway going east towards the residence from 2nd Drive Northeast. There are numerous trees on the SUBJECT PREMISES. There is a wooden post with the numbers 12123 located at the southeast corner of the intersection of 2nd Drive Northeast and the driveway.

The search is to include all rooms, attics, basements, garages, and outbuildings, attached or detached, and any digital device(s) found therein.



1 b. The person to be searched, DAVID PAUL MEATS JR, is a white male
2 who was born on XX/XX/1999.



ATTACHMENT B
ITEMS TO BE SEIZED

The following records, documents, files, or materials, in whatever form, including handmade or mechanical form (such as printed, written, handwritten, or typed), photocopies or other photographic form, and electrical, electronic, and magnetic form (such as CDs, DVDs, smart cards, thumb drives, camera memory cards, electronic notebooks, or any other storage medium), that constitute evidence, instrumentalities, or fruits of violations of 18 U.S.C. § 2252(a)(2) (Receipt or Distribution of Child Pornography) and 18 U.S.C. § 2252(a)(4)(B) (Possession of Child Pornography) which may be found at the SUBJECT PREMISES and on the person of DAVID PAUL MEATS JR (the SUBJECT PERSON).

1. Any visual depiction of minor(s) engaged in sexually explicit conduct, in any format or media.

2. Evidence of any associated email accounts, instant message accounts or other communications or digital storage such as cloud accounts.

3. Letters, e-mail, text messages, and other correspondence identifying persons transmitting child pornography, or evidencing the transmission of child pornography, through interstate or foreign commerce, including by mail or by computer;

4. All invoices, purchase agreements, catalogs, canceled checks, money order receipts, credit card statements or other documents pertaining to the transportation or purchasing of images of minors engaged in sexually explicit conduct;

5. Any and all address books, names, lists of names, telephone numbers, and addresses of individuals engaged in the transfer, exchange, or sale of child pornography;

6. Any and all address books, names, lists of names, telephone numbers, and addresses of minors;

7. Any and all diaries, notebooks, notes, non-pornographic pictures of children, and any other records reflecting personal contact or other activities with minors.

1 8. Any non-digital recording devices and non-digital media capable of storing
2 images and videos.

3 9. Digital devices and/or their components, which include, but are not limited
4 to:

5 a. Any digital devices and storage device capable of being used to
6 commit, further, or store evidence of the offense listed above, including but not limited to
7 computers, digital cameras, and smart phones;

8 b. Any digital devices used to facilitate the transmission, creation,
9 display, encoding or storage of data, including word processing equipment, modems,
10 docking stations, monitors, cameras, printers, encryption devices, and optical scanners;

11 c. Any magnetic, electronic, or optical storage device capable of
12 storing data, such as disks, tapes, CD-ROMs, CD-Rs, CD-RWs, DVDs, printer or
13 memory buffers, smart cards, PC cards, memory sticks, flash drives, thumb drives,
14 camera memory cards, media cards, electronic notebooks, and personal digital assistants;

15 d. Any documentation, operating logs and reference manuals regarding
16 the operation of the digital device or software;

17 e. Any applications, utility programs, compilers, interpreters, and other
18 software used to facilitate direct or indirect communication with the computer hardware,
19 storage devices, or data to be searched;

20 f. Any physical keys, encryption devices, dongles and similar physical
21 items that are necessary to gain access to the computer equipment, storage devices or
22 data; and

23 g. Any passwords, password files, test keys, encryption codes or other
24 information necessary to access the computer equipment, storage devices or data;

25 10. Evidence of who used, owned or controlled any seized digital device(s) at
26 the time the things described in this warrant were created, edited, or deleted, such as logs,
27 registry entries, saved user names and passwords, documents, and browsing history;

1 11. Evidence of malware that would allow others to control any seized digital
2 device(s) such as viruses, Trojan horses, and other forms of malicious software, as well
3 as evidence of the presence or absence of security software designed to detect malware;
4 as well as evidence of the lack of such malware;

5 12. Evidence of the attachment to the digital device(s) of other storage devices
6 or similar containers for electronic evidence;

7 13. Evidence of counter-forensic programs (and associated data) that are
8 designed to eliminate data from a digital device;

9 14. Evidence of times the digital device(s) was used;

10 15. Any other ESI from the digital device(s) necessary to understand how the
11 digital device was used, the purpose of its use, who used it, and when.

12
13 **The seizure of digital devices and/or their components as set forth herein is**
14 **specifically authorized by this search warrant, not only to the extent that such**
15 **digital devices constitute instrumentalities of the criminal activity described above,**
16 **but also for the purpose of the conducting off-site examinations of their contents for**
17 **evidence, instrumentalities, or fruits of the aforementioned crimes. However, if**
18 **executing agents can reasonably determine onsite that the SUBJECT PERSON does**
19 **not own or have access to a particular digital device, they will not seize or search**
20 **that digital device.**
21
22
23
24
25
26
27
28

AFFIDAVIT

STATE OF WASHINGTON
 COUNTY OF KING

ss

I, JASON R. GRAEFF, being duly sworn, state as follows:

INTRODUCTION AND AGENT BACKGROUNDS

1. I am a Special Agent (“SA”) with the Department of Homeland Security (“DHS”), U.S. Immigration and Customs Enforcement (“ICE”), Homeland Security Investigations (“HSI”). I have held such a position since August 2009. HSI is responsible for enforcing the customs and immigration laws and federal criminal statutes of the United States. I am currently assigned to the Office of the Special Agent in Charge (“SAC”), Seattle, Washington, and am a member of the Child Exploitation Investigations Group. As part of my current duties, I investigate criminal violations relating to child exploitation and child pornography, including violations pertaining to the illegal production, distribution, receipt, and possession of child pornography and material involving the sexual exploitation of minors in violation of 18 U.S.C. §§ 2251, 2252, and 2252A. I have received training in investigating child pornography and child exploitation crimes. I have also had the opportunity to observe and review examples of child pornography (as defined in 18 U.S.C. § 2256(8)). I am a member of the Seattle Internet Crimes Against Children Task Force (“ICAC”), and work with other federal, state, and local law enforcement personnel in the investigation and prosecution of crimes involving the sexual exploitation of children.

2. As part of my current duties as an HSI Criminal Investigator, I investigate criminal violations relating to child exploitation and child pornography including violations of Title 18, United States Code, Sections 2251(a), 2252(a)(2), 2252(a)(4)(B), and 2243(a)(1). I have received training in the area of child pornography and child exploitation, and have observed and reviewed numerous examples of child pornography

1 in various forms of media, including media stored on digital media storage devices such
2 as computers, tablets, cellphones, etc. I have also participated in the execution of
3 numerous search warrants involving investigations of child exploitation and/or child
4 pornography offenses. I am a member of the Seattle Internet Crimes Against Children
5 (ICAC) Task Force in the Western District of Washington, and work with other federal,
6 state, and local law enforcement personnel in the investigation and prosecution of crimes
7 involving the sexual exploitation of children. I am a graduate of the Criminal
8 Investigator Training Program ("CITP"), and the ICE Special Agent Training
9 ("ICESAT") at the Federal Law Enforcement Training Center in Glynco, Georgia

10 3. I make this Affidavit in support of an application under Rule 41 of the
11 Federal Rules of Criminal Procedure for a warrant to search:

12 the premises known as 12123 2nd Drive Northeast, Marysville, Washington 98271
13 (the "SUBJECT PREMISES"), and the person of DAVID PAUL MEATS JR (the
14 "SUBJECT PERSON"), more fully described in Attachment A to this Affidavit, for the
15 property and items described in Attachment B to this Affidavit.

16 4. This application seeks a warrant to search SUBJECT PREMISES and the
17 SUBJECT PERSON, and seize the items listed in Attachment B, which is attached to this
18 Affidavit and incorporated herein by reference, for evidence, fruits, and instrumentalities
19 of violations of 18 U.S.C. § 2252(a)(2) (Receipt or Distribution of Child Pornography)
20 and 18 U.S.C. § 2252(a)(4)(B) (Possession of Child Pornography).

21 5. The facts set forth in this Affidavit are based on the following: my own
22 personal knowledge; knowledge obtained from other individuals during my participation
23 in this investigation, including other law enforcement officers; interviews of witnesses;
24 my review of records related to this investigation; communications with others who have
25 knowledge of the events and circumstances described herein; and information gained
26 through my training and experience.

27 6. Because this Affidavit is submitted for the limited purpose of establishing
28 probable cause in support of the application for a search warrant, it does not set forth

1 each and every fact I or others have learned during the course of this investigation. I have
2 set forth only the facts I believe are relevant to the determination of probable cause to
3 believe evidence, fruits, and instrumentalities of violations of 18 U.S.C. § 2252(a)(2)
4 (Receipt or Distribution of Child Pornography) and 18 U.S.C. § 2252(a)(4)(B)
5 (Possession of Child Pornography) will be found in the SUBJECT PREMISES and on the
6 person of DAVID PAUL MEATS JR.

7 This Affidavit is being presented electronically pursuant to Local Criminal Rule
8 CrR 41(d)(3).

9 **KIK MESSENGER AND HASH MATCHING SYSTEM**

10 7. From my training and experience, I know that Kik Messenger, also called
11 KIK, is an instant messenger application (app) for mobile devices from Kik Interactive.
12 KIK is available free of charge on iOS, Android, and Windows Phone operating systems.
13 Among its features, KIK permits users to engage in one-on-one or group chats, as well as
14 share image and video files. KIK is based and headquartered in Waterloo, Ontario,
15 Canada.

16 8. From my training and experience, I am aware that certain KIK users use
17 KIK's features to traffic in images and videos of child pornography. In order to combat
18 this activity, KIK has developed an internal hash matching system called SafePhoto to
19 identify users who are sharing child exploitation material using KIK's services. KIK has
20 created a database of known hash values that it has identified as hash values that
21 correspond to files of known child exploitation material. A hash value can be analogized
22 to a "digital fingerprint." The probability that any two files will have the same hash
23 value is extremely low, meaning that when two files have the same hash value, it is
24 virtually certain that they are identical.

25 9. KIK has a database of approximately 92,000 known child exploitation
26 image hash values, and its system runs a hash value check against every image sent
27 within KIK, including those sent as part of private conversations. When a user sends an
28 image with a hash value that matches a child exploitation hash value in the database, the

1 account is banned. The Trust and Safety team at KIK receives a daily report of all such
 2 hash matches. It has a mandatory obligation to report these matches to the Royal
 3 Canadian Mounted Police (RCMP). With each report, KIK provides some or all of the
 4 following information:

- 5 • Subscriber data associated with the reported user;
- 6 • Full conversation log that exists on the reporter's device, including timestamps
 7 and Internet Protocol (IP) addresses, as well as text content;
- 8 • Images/Videos associated

9 SUMMARY OF INVESTIGATION

10 10. HSI routinely investigates child exploitation leads received from RCMP.
 11 These include leads resulting from the KIK reports to the RCMP described above. KIK
 12 reports to the RCMP all instances where its security team has discovered child
 13 pornography exchanged or discussed via the Kik application. Included in leads, there is
 14 normally profile data of the user, IP connection information, any text transcript if
 15 applicable, and the images shared if any.

16 11. When HSI receives a list of KIK users with IP addresses geolocating in the
 17 United States through this process, it passes those leads along to the appropriate field
 18 office with responsibility for the geographic area associated with a given IP address.

19 12. In February 2019, HSI Seattle received information on the KIK user,
 20 "UNKNOWN_MALE836" (the SUBJECT ACCOUNT). According to the lead, the
 21 SUBJECT ACCOUNT shared an image file with the SHA1 hash value of
 22 868579145DEBDB4EC9C44C4B90AF96B6654645E7 (the SUBJECT FILE) on or
 23 about December 7, 2018, at approximately 06:30:46 Universal Coordinated Time (UTC)
 24 from the IP address 199.30.252.22 (the SUBJECT IP). The hash value of the SUBJECT
 25 FILE was identified via SafePhoto as a known child exploitation image hash file.
 26 Information provided by KIK shows that the user of the SUBJECT ACCOUNT used an
 27 iPhone while accessing the application, and IP log data showed IP addresses belonging to
 28 multiple ISPs were used to connect to the SUBJECT ACCOUNT, including AT&T

1 wireless and Salish Networks, Inc. The user of the account also supplied an email
2 address, davidmeats1999@gmail.com.

3 13. On or about March 8, 2019, SA Huynh applied for and obtained a federal
4 search warrant (MJ19-095) signed by the honorable Mary Alice Theiler of the Western
5 District of Washington granting the authority to open and view the SUBJECT FILE.

6 14. SA Huynh subsequently opened and viewed the SUBJECT FILE. I have
7 not examined the SUBJECT FILE and am not relying on SA Huynh's observations or
8 conclusions about its content for purposes of this warrant application.

9 15. SA Huynh asked the HSI Cyber Crimes Center (C3) to determine whether
10 the hash value for the SUBJECT FILE provided by KIK is a known has value—meaning
11 a hash value associated with a child exploitation file previously seen by law enforcement.
12 According to C3, the hash value of the SUBJECT FILE corresponds to an image
13 depicting an identified minor victim known to the National Center for Missing and
14 Exploited Children (NCMEC). An image file with the same hash value as the SUBJECT
15 FILE is on file with the HSI child exploitation imagery repository. C3 provided me with
16 a copy of this image (the REPOSITORY FILE). As noted above, because the SUBJECT
17 FILE and the REPOSITORY FILE share the same hash value, it is virtually impossible
18 for these files not to be identical.

19 16. I viewed the REPOSITORY FILE obtained from C3 and describe it below:
20 This is a color photograph depicting a prepubescent female lying on her back. Her
21 legs are spread, and she is nude from the waist down, exposing her genitals to the
22 camera. The left hand of an adult is resting on the minor's inner thigh, and the
23 adult's thumb is pressed against the outside of the minor's genitals. The minor is
24 also being anally penetrated by an erect penis. Based on her stature and size in
25 comparison to the adult hand and lack of pubic hair and pubic development, it
26 appears the minor is under the age of four.

27 17. I determined that the SUBJECT IP from which the SUBJECT FILE was
28 uploaded belongs to Salish Networks, Inc.

18. In response to a summons seeking subscriber information for the SUBJECT IP at the time the SUBJECT FILE was uploaded to KIK, Salish Networks, Inc., reported that the SUBJECT IP was assigned to subscriber C.C. with the service address 12123 2nd Dr NE Tulalip WA 98271 (the SUBJECT PREMISES) at the time the SUBJECT FILE was uploaded to KIK.

19. Travel records for C.C. show that he traveled to China in the summer of 2018. These records show he was accompanied by S.C. and DAVID PAUL MEATS JR (DOB: XX/XX/1999) (the SUBJECT PERSON). As noted above, the user of the SUBJECT ACCOUNT provided an email address of davidmeats1999@gmail.com, suggesting that the SUBJECT PERSON is the user of the SUBJECT ACCOUNT.

20. Washington State Department of Licensing checks revealed identification/driver's licenses linked to the SUBJECT PERSON that list the SUBJECT PREMISES as his address. These same records show driver's licenses for at least five other individuals that list the SUBJECT PREMISES as an address.

21. Records checks also show that the SUBJECT PERSON provided the email address davidmeats1999@gmail.com in a recent U.S. passport application.

TECHNICAL BACKGROUND

22. Based on my training and experience, when an individual communicates through the Internet, the individual leaves an IP address which identifies the individual user by account and ISP (as described above). When an individual is using the Internet, the individual's IP address is visible to administrators of websites they visit. Further, the individual's IP address is broadcast during most Internet file and information exchanges that occur.

23. Based on my training and experience, I know that most ISPs provide only one IP address for each residential subscription. I also know that individuals often use multiple digital devices within their home to access the Internet, including desktop and laptop computers, tablets, and mobile phones. A device called a router is used to connect multiple digital devices to the Internet via the public IP address assigned (to the

1 subscriber) by the ISP. A wireless router performs the functions of a router but also
2 includes the functions of a wireless access point, allowing (wireless equipped) digital
3 devices to connect to the Internet via radio waves, not cables. Based on my training and
4 experience, today many residential Internet customers use a wireless router to create a
5 computer network within their homes where users can simultaneously access the Internet
6 (with the same public IP address) with multiple digital devices.

7 24. Based on my training and experience and information provided to me by
8 computer forensic agents, I know that data can quickly and easily be transferred from one
9 digital device to another digital device. Data can be transferred from computers or other
10 digital devices to internal and/or external hard drives, tablets, mobile phones, and other
11 mobile devices via a USB cable or other wired connection. Data can also be transferred
12 between computers and digital devices by copying data to small, portable data storage
13 devices including USB (often referred to as “thumb”) drives, memory cards (Compact
14 Flash, SD, microSD, etc.) and memory card readers, and optical discs (CDs/DVDs).

15 25. As outlined above, residential Internet users can simultaneously access the
16 Internet in their homes with multiple digital devices. Also explained above is how data
17 can quickly and easily be transferred from one digital device to another through the use
18 of wired connections (hard drives, tablets, mobile phones, etc.) and portable storage
19 devices (USB drives, memory cards, optical discs). Therefore, a user could access the
20 Internet using their assigned public IP address, receive, transfer or download data, and
21 then transfer that data to other digital devices, which may or may not have been
22 connected to the Internet during the date and time of the specified transaction.

23 26. Based on my training and experience, I have learned that the computer’s
24 ability to store images and videos in digital form makes the computer itself an ideal
25 repository for child pornography. The size of hard drives used in computers (and other
26 digital devices) has grown tremendously within the last several years. Hard drives with
27 the capacity of four (4) terabytes (TB) are not uncommon. These drives can store
28 thousands of images and videos at very high resolution.

1 27. Based on my training and experience, and information provided to me by
2 other law enforcement officers, I know that people tend to use the same user names
3 across multiple accounts and email services.

4 28. Based on my training and experience, collectors and distributors of child
5 pornography also use online resources to retrieve and store child pornography, including
6 services offered by companies such as Google, Yahoo, Apple, and Dropbox, among
7 others. The online services allow a user to set up an account with a remote computing
8 service that provides email services and/or electronic storage of computer files in any
9 variety of formats. A user can set up an online storage account from any computer with
10 access to the Internet. Evidence of such online storage of child pornography is often
11 found on the user's computer. Even in cases where online storage is used, however,
12 evidence of child pornography can be found on the user's computer in most cases.

13 29. As is the case with most digital technology, communications by way of
14 computer can be saved or stored on the computer used for these purposes. Storing this
15 information can be intentional, i.e., by saving an email as a file on the computer or saving
16 the location of one's favorite websites in, for example, "bookmarked" files. Digital
17 information can also be retained unintentionally, e.g., traces of the path of an electronic
18 communication may be automatically stored in many places (e.g., temporary files or ISP
19 client software, among others). In addition to electronic communications, a computer
20 user's Internet activities generally leave traces or "footprints" and history files of the
21 browser application used. A forensic examiner often can recover evidence suggesting
22 whether a computer contains wireless software, and when certain files under investigation
23 were uploaded or downloaded. Such information is often maintained indefinitely until
24 overwritten by other data.

25 30. Based on my training and experience, I have learned that producers of child
26 pornography can produce image and video digital files from the average digital camera,
27 mobile phone, or tablet. These files can then be easily transferred from the mobile device
28 to a computer or other digital device, using the various methods described above. The

1 digital files can then be stored, manipulated, transferred, or printed directly from a
2 computer or other digital device. Digital files can also be edited in ways similar to those
3 by which a photograph may be altered; they can be lightened, darkened, cropped, or
4 otherwise manipulated. As a result of this technology, it is relatively inexpensive and
5 technically easy to produce, store, and distribute child pornography. In addition, there is
6 an added benefit to the child pornographer in that this method of production is a difficult
7 trail for law enforcement to follow.

8 31. As part of my training and experience, I have become familiar with the
9 structure of the Internet, and I know that connections between computers on the Internet
10 routinely cross state and international borders, even when the computers communicating
11 with each other are in the same state. Individuals and entities use the Internet to gain
12 access to a wide variety of information; to send information to, and receive information
13 from, other individuals; to conduct commercial transactions; and to communicate via
14 email.

15 32. Based on my training and experience, I know that cellular mobile phones
16 (often referred to as "smart phones") have the capability to access the Internet and store
17 information, such as images and videos. As a result, an individual using a smart phone
18 can send, receive, and store files, including child pornography, without accessing a
19 personal computer or laptop. An individual using a smart phone can also easily connect
20 the device to a computer or other digital device, via a USB or similar cable, and transfer
21 data files from one digital device to another. Moreover, many media storage devices,
22 including smartphones and thumb drives, can easily be concealed and carried on an
23 individual's person and smartphones and/or mobile phones are also often carried on an
24 individual's person.

25 33. As set forth herein and in Attachment B to this Affidavit, I seek permission
26 to search for and seize evidence, fruits, and instrumentalities of the above-referenced
27 crimes that might be found at the SUBJECT PREMISES or on the SUBJECT PERSON,
28 in whatever form they are found. It has been my experience that individuals involved in

1 child pornography often prefer to store images of child pornography in electronic form.
2 The ability to store images of child pornography in electronic form makes digital devices,
3 examples of which are enumerated in Attachment B to this Affidavit, an ideal repository
4 for child pornography because the images can be easily sent or received over the Internet.
5 As a result, one form in which these items may be found is as electronic evidence stored
6 on a digital device.

7 34. Based upon my knowledge, experience, and training in child pornography
8 investigations, and the training and experience of other law enforcement officers with
9 whom I have had discussions, I know that there are certain characteristics common to
10 individuals who have a sexualized interest in children and depictions of children:

11 a. They may receive sexual gratification, stimulation, and satisfaction
12 from contact with children; or from fantasies they may have viewing children engaged in
13 sexual activity or in sexually suggestive poses, such as in person, in photographs, or other
14 visual media; or from literature describing such activity.

15 b. They may collect sexually explicit or suggestive materials in a
16 variety of media, including photographs, magazines, motion pictures, videotapes, books,
17 slides, and/or drawings or other visual media. Such individuals often times use these
18 materials for their own sexual arousal and gratification. Further, they may use these
19 materials to lower the inhibitions of children they are attempting to seduce, to arouse the
20 selected child partner, or to demonstrate the desired sexual acts. These individuals may
21 keep records, to include names, contact information, and/or dates of these interactions, of
22 the children they have attempted to seduce, arouse, or with whom they have engaged in
23 the desired sexual acts.

24 c. They often maintain any “hard copies” of child pornographic
25 material that is, their pictures, films, video tapes, magazines, negatives, photographs,
26 correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of
27 their home or some other secure location. These individuals typically retain these “hard
28 copies” of child pornographic material for many years, as they are highly valued.

1 d. Likewise, they often maintain their child pornography collections
2 that are in a digital or electronic format in a safe, secure and private environment, such as
3 a computer and surrounding area. These collections are often maintained for several
4 years and are kept close by, often at the individual's residence or some otherwise easily
5 accessible location, to enable the owner to view the collection, which is valued highly.

6 e. They also may correspond with and/or meet others to share
7 information and materials; rarely destroy correspondence from other child pornography
8 distributors/collectors; conceal such correspondence as they do their sexually explicit
9 material; and often maintain lists of names, addresses, and telephone numbers of
10 individuals with whom they have been in contact and who share the same interests in
11 child pornography.

12 f. They generally prefer not to be without their child pornography for
13 any prolonged time period. This behavior has been documented by law enforcement
14 officers involved in the investigation of child pornography throughout the world.

15 g. E-mail itself provides a convenient means by which individuals can
16 access a collection of child pornography from any computer, at any location with Internet
17 access. Such individuals therefore do not need to physically carry their collections with
18 them but rather can access them electronically. Furthermore, these collections can be
19 stored on email "cloud" servers, which allow users to store a large amount of material at
20 no cost, without leaving any physical evidence on the users' computer(s).

21 35. In addition to offenders who collect and store child pornography, law
22 enforcement has encountered offenders who obtain child pornography from the internet,
23 view the contents and subsequently delete the contraband, often after engaging in self-
24 gratification. In light of technological advancements, increasing Internet speeds and
25 worldwide availability of child sexual exploitative material, this phenomenon offers the
26 offender a sense of decreasing risk of being identified and/or apprehended with quantities
27 of contraband. This type of consumer is commonly referred to as a 'seek and delete'
28 offender, knowing that the same or different contraband satisfying their interests remain

1 easily discoverable and accessible online for future viewing and self-gratification. I
2 know that, regardless of whether a person discards or collects child pornography he/she
3 accesses for purposes of viewing and sexual gratification, evidence of such activity is
4 likely to be found on computers and related digital devices, including storage media, used
5 by the person. This evidence may include the files themselves, logs of account access
6 events, contact lists of others engaged in trafficking of child pornography, backup files,
7 and other electronic artifacts that may be forensically recoverable.

8 36. Given the above-stated facts and based on my knowledge, training and
9 experience, along with my discussions with other law enforcement officers who
10 investigate child exploitation crimes, I believe that the SUBJECT PERSON has a
11 sexualized interest in children and depictions of children and that evidence of child
12 pornography is likely to be found on digital media devices, including mobile and/or
13 portable digital devices found at the SUBJECT PREMISES or on the SUBJECT
14 PERSON.

15 37. Based on my training and experience, and that of computer forensic agents
16 that I work and collaborate with on a daily basis, I know that every type and kind of
17 information, data, record, sound or image can exist and be present as electronically stored
18 information on any of a variety of computers, computer systems, digital devices, and
19 other electronic storage media. I also know that electronic evidence can be moved easily
20 from one digital device to another. As a result, I believe that electronic evidence may be
21 stored on any digital device present at the SUBJECT PREMISES or on the SUBJECT
22 PERSON.

23 38. Based on my training and experience, and my consultation with computer
24 forensic agents who are familiar with searches of computers, I know that in some cases
25 the items set forth in Attachment B may take the form of files, documents, and other data
26 that is user-generated and found on a digital device. In other cases, these items may take
27 the form of other types of data - including in some cases data generated automatically by
28 the devices themselves.

1 39. Based on my training and experience, and my consultation with computer
2 forensic agents who are familiar with searches of computers, I believe that if digital
3 devices are found in the SUBJECT PREMISES or on the SUBJECT PERSON, there is
4 probable cause to believe that the items set forth in Attachment B will be stored in those
5 digital devices for a number of reasons, including but not limited to the following:

6 a. Once created, electronically stored information (ESI) can be stored
7 for years in very little space and at little or no cost. A great deal of ESI is created, and
8 stored, moreover, even without a conscious act on the part of the device operator. For
9 example, files that have been viewed via the Internet are sometimes automatically
10 downloaded into a temporary Internet directory or "cache," without the knowledge of the
11 device user. The browser often maintains a fixed amount of hard drive space devoted to
12 these files, and the files are only overwritten as they are replaced with more recently
13 viewed Internet pages or if a user takes affirmative steps to delete them. This ESI may
14 include relevant and significant evidence regarding criminal activities, but also, and just
15 as importantly, may include evidence of the identity of the device user, and when and
16 how the device was used. Most often, some affirmative action is necessary to delete ESI.
17 And even when such action has been deliberately taken, ESI can often be recovered,
18 months or even years later, using forensic tools.

19 b. Wholly apart from data created directly (or indirectly) by user
20 generated files, digital devices - in particular, a computer's internal hard drive - contain
21 electronic evidence of how a digital device has been used, what it has been used for, and
22 who has used it. This evidence can take the form of operating system configurations,
23 artifacts from operating systems or application operations, file system data structures, and
24 virtual memory "swap" or paging files. Computer users typically do not erase or delete
25 this evidence, because special software is typically required for that task. However, it is
26 technically possible for a user to use such specialized software to delete this type of
27 information - and, the use of such special software may itself result in ESI that is relevant
28 to the criminal investigation. In particular, to properly retrieve and analyze electronically

1 stored (computer) data, and to ensure accuracy and completeness of such data and to
2 prevent loss of the data either from accidental or programmed destruction, it is necessary
3 to conduct a forensic examination of the computers. To effect such accuracy and
4 completeness, it may also be necessary to analyze not only data storage devices, but also
5 peripheral devices which may be interdependent, the software to operate them, and
6 related instruction manuals containing directions concerning operation of the computer
7 and software.

8 **SEARCH AND/OR SEIZURE OF DIGITAL DEVICES**

9 40. In addition, based on my training and experience and that of computer
10 forensic agents that I work and collaborate with on a daily basis, I know that in most
11 cases it is impossible to successfully conduct a complete, accurate, and reliable search for
12 electronic evidence stored on a digital device during the physical search of a search site
13 for a number of reasons, including but not limited to the following:

14 a. Technical Requirements: Searching digital devices for criminal
15 evidence is a highly technical process requiring specific expertise and a properly
16 controlled environment. The vast array of digital hardware and software available
17 requires even digital experts to specialize in particular systems and applications, so it is
18 difficult to know before a search which expert is qualified to analyze the particular
19 system(s) and electronic evidence found at a search site. As a result, it is not always
20 possible to bring to the search site all of the necessary personnel, technical manuals, and
21 specialized equipment to conduct a thorough search of every possible digital
22 device/system present. In addition, electronic evidence search protocols are exacting
23 scientific procedures designed to protect the integrity of the evidence and to recover even
24 hidden, erased, compressed, password-protected, or encrypted files. Since ESI is
25 extremely vulnerable to inadvertent or intentional modification or destruction (both from
26 external sources or from destructive code embedded in the system such as a "booby
27 trap"), a controlled environment is often essential to ensure its complete and accurate
28 analysis.

1 b. Volume of Evidence: The volume of data stored on many digital
2 devices is typically so large that it is impossible to search for criminal evidence in a
3 reasonable period of time during the execution of the physical search of a search site. A
4 single megabyte of storage space is the equivalent of 500 double-spaced pages of text. A
5 single gigabyte of storage space, or 1,000 megabytes, is the equivalent of 500,000
6 double-spaced pages of text. Computer hard drives are now being sold for personal
7 computers capable of storing up to two terabytes (2,000 gigabytes of data.) Additionally,
8 this data may be stored in a variety of formats or may be encrypted (several new
9 commercially available operating systems provide for automatic encryption of data upon
10 shutdown of the computer).

11 c. Search Techniques: Searching the ESI for the items described in
12 Attachment B may require a range of data analysis techniques. In some cases, it is
13 possible for agents and analysts to conduct carefully targeted searches that can locate
14 evidence without requiring a time-consuming manual search through unrelated materials
15 that may be commingled with criminal evidence. In other cases, however, such
16 techniques may not yield the evidence described in the warrant, and law enforcement
17 personnel with appropriate expertise may need to conduct more extensive searches, such
18 as scanning areas of the disk not allocated to listed files, or peruse every file briefly to
19 determine whether it falls within the scope of the warrant.

20 41. In this particular case, the government anticipates the use of a hash value
21 library to exclude normal operating system files that do not need to be searched, which
22 will facilitate the search for evidence that does come within the items described in
23 Attachment B. Further, the government anticipates the use of hash values and known file
24 filters to assist the digital forensics examiners/agents in identifying known and or
25 suspected child pornography image files. Use of these tools will allow for the quick
26 identification of evidentiary files but also assist in the filtering of normal system files that
27 would have no bearing on the case.
28

1 42. Collectors of child pornography are known to transport their child
2 pornography collections, which are often stored on mobile and/or portable digital media
3 devices, with them throughout the day. In particular, I have consulted with law
4 enforcement officers with experience investigating child exploitation related crimes, and
5 have learned that collectors of child pornography have been found to transport their
6 collections stored on mobile and/or portable devices 1) within pockets on their person,
7 and 2) inside bags/backpacks that they carry, and/or 3) within compartments located
8 inside their vehicle.

9 43. Because multiple people share the SUBJECT PREMISES and in order to
10 protect the privacy of individuals who may not be suspects of criminal activity, executing
11 agents will attempt to determine onsite which resident or residents own or have access to
12 a given digital device. If executing agents can reasonably determine onsite that the
13 SUBJECT PERSON does not own or have access to a particular digital device, they will
14 not seize or search that digital device.

15 44. In accordance with the information in this Affidavit, law enforcement
16 personnel will execute the search of digital devices seized pursuant to this warrant as
17 follows:

18 a. Upon securing the search site, the search team will conduct an initial
19 review of any digital devices/systems to determine whether the ESI contained therein can
20 be searched and/or duplicated on site in a reasonable amount of time and without
21 jeopardizing the ability to accurately preserve the data.

22 b. If, based on their training and experience, and the resources
23 available to them at the search site, the search team determines it is not practical to make
24 an on-site search, or to make an on-site copy of the ESI within a reasonable amount of
25 time and without jeopardizing the ability to accurately preserve the data, then the digital
26 devices will be seized and transported to an appropriate law enforcement laboratory for
27 review and to be forensically copied ("imaged"), as appropriate.
28

1 c. In order to examine the ESI in a forensically sound manner, law
2 enforcement personnel with appropriate expertise will produce a complete forensic
3 image, if possible and appropriate, of any digital device that is found to contain data or
4 items that fall within the scope of Attachment B of this Affidavit. In addition,
5 appropriately trained personnel may search for and attempt to recover deleted, hidden, or
6 encrypted data to determine whether the data fall within the list of items to be seized
7 pursuant to the warrant. In order to search fully for the items identified in the warrant,
8 law enforcement personnel, which may include investigative agents, may then examine
9 all of the data contained in the forensic image/s and/or on the digital devices to view their
10 precise contents and determine whether the data fall within the list of items to be seized
11 pursuant to the warrant.

12 d. The search techniques that will be used will be only those
13 methodologies, techniques and protocols as may reasonably be expected to find, identify,
14 segregate and/or duplicate the items authorized to be seized pursuant to Attachment B to
15 this Affidavit.

16 e. If, after conducting its examination, law enforcement personnel
17 determine that any digital device is an instrumentality of the criminal offenses referenced
18 above, the government may retain that device during the pendency of the case as
19 necessary to, among other things, preserve the instrumentality evidence for trial, ensure
20 the chain of custody, and litigate the issue of forfeiture. If law enforcement personnel
21 determine that a device was not an instrumentality of the criminal offenses referenced
22 above, it shall be returned to the person/entity from whom it was seized within 90 days of
23 the issuance of the warrant, unless the government seeks and obtains authorization from
24 the court for its retention.

25 45. In order to search for ESI that falls within the list of items to be seized
26 pursuant to Attachment B to this Affidavit, law enforcement personnel will seize and
27 search the following items (heretofore and hereinafter referred to as "digital devices"),
28 subject to the procedures set forth above:

1 a. Any digital device capable of being used to commit, further, or store
2 evidence of the offense(s) listed above;

3 b. Any digital device used to facilitate the transmission, creation,
4 display, encoding, or storage of data, including word processing equipment, modems,
5 docking stations, monitors, printers, cameras, encryption devices, and optical scanners;

6 c. Any magnetic, electronic, or optical storage device capable of
7 storing data, such as disks, tapes, CD-ROMs, CD-Rs, CD-RWs, DVDs, printer or
8 memory buffers, smart cards, PC cards, memory sticks, flash drives, thumb drives,
9 camera memory cards, media cards, electronic notebooks, and personal digital assistants;

10 d. Any documentation, operating logs and reference manuals regarding
11 the operation of the digital device, or software;

12 e. Any applications, utility programs, compilers, interpreters, and other
13 software used to facilitate direct or indirect communication with the device hardware, or
14 ESI to be searched;

15 f. Any physical keys, encryption devices, dongles and similar physical
16 items that are necessary to gain access to the digital device, or ESI; and


17 g. Any passwords, password files, test keys, encryption codes or other
18 information necessary to access the digital device or ESI.

19 **GENUINE RISKS OF DESTRUCTION OF EVIDENCE**


20 46. Any other means of obtaining the necessary evidence to prove the elements
21 of computer/Internet-related crimes, for example, a consent search, could result in an
22 unacceptable risk of the loss/destruction of the evidence sought. If agents pursued a
23 consent-based interview of and/or a consent-based search of digital media belonging to
24 DAVID PAUL MEATS JR at the SUBJECT PREMISES, he could rightfully refuse to
25 give consent and subsequently destroy all evidence of the crime before agents could
26 return with a search warrant. Based on my knowledge, training and experience, the only
27 effective means of collecting and preserving the required evidence in this case is through
28 a search warrant.

CONCLUSION

47. Based on the foregoing, I believe there is probable cause that evidence, fruits, and instrumentalities of violations of 18 U.S.C. § 2252(a)(2) (Receipt or Distribution of Child Pornography) and 18 U.S.C. § 2252(a)(4)(B) (Possession of Child Pornography) are located at the SUBJECT PREMISES, as more fully described in Attachment A to this Affidavit, as well as on and in any digital devices found therein. I therefore request that the court issue a warrant authorizing a search of the SUBJECT PREMISES and on the person of DAVID PAUL MEATS JR for the items more fully described in Attachment B hereto, incorporated herein by reference, and the seizure of any such items found therein.


JASON R. GRAEFF,
Affiant, Special Agent
Department of Homeland Security
Homeland Security Investigations

The above-named agent provided a sworn statement attesting to the truth of the contents of the foregoing affidavit on the 12th day of April, 2019.


BRIAN A. TSUCHIDA
Chief United States Magistrate Judge

ATTACHMENT A**Description of the Property to be Searched**

a. The physical address of the SUBJECT PREMISES is 12123 2nd Drive Northeast, Marysville (Tulalip), Washington 98271 . The SUBJECT PREMISES is more fully described as the property containing a one-story single-family home with a daylight basement. The Snohomish County Assessor's and Google Earth web search of the property reveal that the residence structure appears to have a first or main story that is approximately 2614 square feet with the basement or daylight basement of 2616 square feet. There is a three-car garage located to the right of the main door or at the southwest corner of the residence. The Snohomish County Assessor lists the garage being approximately 864 square feet. Google Earth shows the daylight basement with possible access to the backyard located on the east side of the residence. There appears to be a large deck coming out from the main floor. The SUBJECT PREMISES is located at the east side of 2nd Drive Northeast. The SUBJECT PREMISES has a long driveway going east towards the residence from 2nd Drive Northeast. There are numerous trees on the SUBJECT PREMISES. There is a wooden post with the numbers 12123 located at the southeast corner of the intersection of 2nd Drive Northeast and the driveway.

The search is to include all rooms, attics, basements, garages, and outbuildings, attached or detached, and any digital device(s) found therein.



1 b. The person to be searched, DAVID PAUL MEATS JR, is a white male
2 who was born on XX/XX/1999.



ATTACHMENT B
ITEMS TO BE SEIZED

The following records, documents, files, or materials, in whatever form, including handmade or mechanical form (such as printed, written, handwritten, or typed), photocopies or other photographic form, and electrical, electronic, and magnetic form (such as CDs, DVDs, smart cards, thumb drives, camera memory cards, electronic notebooks, or any other storage medium), that constitute evidence, instrumentalities, or fruits of violations of 18 U.S.C. § 2252(a)(2) (Receipt or Distribution of Child Pornography) and 18 U.S.C. § 2252(a)(4)(B) (Possession of Child Pornography) which may be found at the SUBJECT PREMISES and on the person of DAVID PAUL MEATS JR (the SUBJECT PERSON).

1. Any visual depiction of minor(s) engaged in sexually explicit conduct, in any format or media.

2. Evidence of any associated email accounts, instant message accounts or other communications or digital storage such as cloud accounts.

3. Letters, e-mail, text messages, and other correspondence identifying persons transmitting child pornography, or evidencing the transmission of child pornography, through interstate or foreign commerce, including by mail or by computer;

4. All invoices, purchase agreements, catalogs, canceled checks, money order receipts, credit card statements or other documents pertaining to the transportation or purchasing of images of minors engaged in sexually explicit conduct;

5. Any and all address books, names, lists of names, telephone numbers, and addresses of individuals engaged in the transfer, exchange, or sale of child pornography;

6. Any and all address books, names, lists of names, telephone numbers, and addresses of minors;

7. Any and all diaries, notebooks, notes, non-pornographic pictures of children, and any other records reflecting personal contact or other activities with minors.

1 8. Any non-digital recording devices and non-digital media capable of storing
2 images and videos.

3 9. Digital devices and/or their components, which include, but are not limited
4 to:

5 a. Any digital devices and storage device capable of being used to
6 commit, further, or store evidence of the offense listed above, including but not limited to
7 computers, digital cameras, and smart phones;

8 b. Any digital devices used to facilitate the transmission, creation,
9 display, encoding or storage of data, including word processing equipment, modems,
10 docking stations, monitors, cameras, printers, encryption devices, and optical scanners;

11 c. Any magnetic, electronic, or optical storage device capable of
12 storing data, such as disks, tapes, CD-ROMs, CD-Rs, CD-RWs, DVDs, printer or
13 memory buffers, smart cards, PC cards, memory sticks, flash drives, thumb drives,
14 camera memory cards, media cards, electronic notebooks, and personal digital assistants;

15 d. Any documentation, operating logs and reference manuals regarding
16 the operation of the digital device or software;

17 e. Any applications, utility programs, compilers, interpreters, and other
18 software used to facilitate direct or indirect communication with the computer hardware,
19 storage devices, or data to be searched;

20 f. Any physical keys, encryption devices, dongles and similar physical
21 items that are necessary to gain access to the computer equipment, storage devices or
22 data; and

23 g. Any passwords, password files, test keys, encryption codes or other
24 information necessary to access the computer equipment, storage devices or data;

25 10. Evidence of who used, owned or controlled any seized digital device(s) at
26 the time the things described in this warrant were created, edited, or deleted, such as logs,
27 registry entries, saved user names and passwords, documents, and browsing history;

1 11. Evidence of malware that would allow others to control any seized digital
2 device(s) such as viruses, Trojan horses, and other forms of malicious software, as well
3 as evidence of the presence or absence of security software designed to detect malware;
4 as well as evidence of the lack of such malware;

5 12. Evidence of the attachment to the digital device(s) of other storage devices
6 or similar containers for electronic evidence;

7 13. Evidence of counter-forensic programs (and associated data) that are
8 designed to eliminate data from a digital device;

9 14. Evidence of times the digital device(s) was used;

10 15. Any other ESI from the digital device(s) necessary to understand how the
11 digital device was used, the purpose of its use, who used it, and when.

12
13 **The seizure of digital devices and/or their components as set forth herein is**
14 **specifically authorized by this search warrant, not only to the extent that such**
15 **digital devices constitute instrumentalities of the criminal activity described above,**
16 **but also for the purpose of the conducting off-site examinations of their contents for**
17 **evidence, instrumentalities, or fruits of the aforementioned crimes. However, if**
18 **executing agents can reasonably determine onsite that the SUBJECT PERSON does**
19 **not own or have access to a particular digital device, they will not seize or search**
20 **that digital device.**
21
22
23
24
25
26
27
28